Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

Claim 1 (currently amended): A method of providing from a centralized location access control to a resource for one or more users, said method comprising:

receiving at the centralized location an authorization request from a first entity to issue authorization data for the one or more users based on roles associated with the users as part of an organization model, wherein said authorization data is required by a second entity for allowing the first entity to conditionally access a resource controlled by the second entity;

responsive to the received authorization request, issuing the authorization data from the centralized location to the first entity, wherein the first entity provides the issued authorization data to the second entity to conditionally access the resource controlled by the second entity, said authorization data including [[an]] a conditional scope expression identifying the resource by a resource name and by at least one property name-property value pair associated with the resource to conditionally define access to the resource, said property name-property value pair determining a list of conditions for access to the resource controlled by the second entity, said authorization data further including validation information;

receiving at the centralized location a validation request from the second entity to validate the issued authorization data ~~that was~~ provided to the second entity by the first entity; ~~and~~

responsive to the received validation request, validating the issued authorization data based on the validation information included ~~there~~in the authorization data; and

responsive to validating the issued authorization data, sending from the centralized location a response to the second entity indicating a determined validation status ~~responsive to said validating the issued authorization data~~, said second entity granting to the first entity access to the resource according to the conditions determined by the property name-property value pair when the determined validation status indicates that the authorization data is valid.

Claim 2 (canceled).

Claim 3 (canceled).

Claim 4 (previously presented): The method of claim 1, wherein receiving the requests and issuing the authorization data occur over a secure sockets layer.

Claim 5 (previously presented): The method of claim 1, wherein receiving the requests and issuing the authorization data occur over a network such as the Internet.

Claim 6 (currently amended): The method of claim 1, further comprising creating the conditional scope expression identifying the resource in response to the received authorization request.

Claim 7 (currently amended): The method of claim 6, further comprising encrypting the created conditional scope expression.

Claim 8 (canceled).

Claim 9 (canceled).

Claim 10 (currently amended): The method of claim 1, wherein one or more computer-readable storage media ~~have~~ having stored thereon computer-executable instructions for performing the method of claim 1.

Claim 11 (currently amended): A method for validating at a centralized location authorization data to provide conditional access to a resource for one or more users, said method comprising:

receiving at the centralized location an authorization request from a client to issue authorization data for the one or more users based on roles associated with the users, wherein

said authorization data is required by an affiliate server for allowing the client to conditionally access a resource controlled by said affiliate server;

responsive to the received authorization request, generating at the centralized location an authorization token having a header field, a source field, and a claim field, said header field representing validation information, said source field representing the identity of the user, said claim field specifying the resource conditionally, said claim field including [[an]] a conditional scope expression identifying the resource by a resource name and by at least one property name-property value pair associated with the resource to conditionally define access to the resource, said property name-property value pair determining a list of conditions for access to the resource controlled by the affiliate server;

sending the authorization token from the centralized location to the client, wherein the client provides the authorization token to the affiliate server to conditionally access the resource controlled by the affiliate server;

receiving at the centralized location over a secure sockets layer a validation request from the affiliate server to validate the authorization token provided by the client, said receiving the validation request comprises receiving a data packet according to the Simple Object Access Protocol (SOAP), and further comprising extracting the authorization token from the received data packet;

responsive to the extracted authorization token, retrieving validation information from the header field of the received authorization token;

responsive to the retrieved validation information, evaluating the retrieved validation information to determine a validation status of the received authorization token; and

responsive to the determined validation status, sending from the centralized location a response to the affiliate server indicating [[a]] the determined validation status, said affiliate server granting to the client access to the resource according to the conditions determined by the property name-property value pair when the determined validation status indicates that the authorization token is valid ~~responsive to said evaluating the retrieved validation information~~.

Claim 12 (currently amended): The method of claim 11, further comprising evaluating the conditional scope expression to identify the resource.

Claim 13 (currently amended): The method of claim 12, wherein evaluating the conditional scope expression comprises extracting a target scope from the received authorization token, said extracted target scope identifying the resource.

Claim 14 (canceled).

Claim 15 (canceled).

Claim 16 (previously presented): The method of claim 11, wherein receiving the validation request including the authorization token occurs over a network such as the Internet.

Claim 17 (previously presented): The method of claim 11, further comprising decrypting the received authorization token.

Claim 18 (canceled).

Claim 19 (previously presented): The method of claim 11, wherein retrieving the validation information comprises retrieving a signature from the header of the received authorization token.

Claim 20 (previously presented): The method of claim 19, wherein evaluating the retrieved validation information comprises determining that the retrieved signature is invalid, and wherein sending the response comprises sending a response indicating the invalidity of the received authorization token.

Claim 21 (previously presented): The method of claim 11, wherein retrieving the validation information comprises retrieving an expiration date from the header of the received authorization token, and wherein evaluating the retrieved validation information comprises comparing the retrieved expiration date to a current time stamp to determine if the received authorization token has expired.

Claim 22 (previously presented): The method of claim 21, wherein the received authorization token has been determined to be expired, and further comprising sending a response indicating the invalidity of the received authorization token.

Claim 23 (currently amended): The method of claim 11, wherein one or more computer-readable storage media ~~have~~ having stored thereon computer-executable instructions for performing the method recited in claim 11.

Claim 24 (currently amended): One or more computer-readable media having stored thereon computer-executable components to control access to a resource by one or more users from a centralized location, said components comprising:

an interface component adapted to receive at the centralized location an authorization request from a first entity to issue authorization data for the one or more users based on roles associated with the users, wherein said authorization data is required by a second entity for allowing the client to conditionally access a resource controlled by said second entity;

an authorization component adapted to issue at the centralized location the requested authorization data for the users based on the roles associated with the users to the first entity, said authorization data including [[an] a conditional scope expression identifying a resource by a resource name and by at least one [[a]] property name-property value pair associated with the resource, said property name-property value pair determining a list of conditions for access to the resource controlled by the second entity, and said authorization data including the validation information, wherein said interface component is further adapted to receive a validation request from the second entity, said validation request including the authorization data issued to the first entity;

a parser component adapted to retrieve validation information from the received authorization data; and

a validation component adapted to evaluate the retrieved validation information, wherein the interface component is further adapted to send a response from the centralized location to the second entity indicating a validation status of the received authorization data responsive to said evaluating the retrieved validation information, said second entity granting to the first entity

access to the resource according to the conditions determined by the property name-property value pair when the determined validation status indicates that the authorization data is valid.

Claim 25 (canceled).

Claim 26 (canceled).

Claim 27 (currently amended): The computer-readable media of claim 24, further comprising a scope component to evaluate the conditional scope expression to identify the resource.

Claim 28 (currently amended): An authorization system in a centralized location comprising:

a memory area accessible from the centralized location for storing authorization data for use in providing a first entity conditional access to a resource that is controlled by a second entity, said authorization data including [[an]] a conditional scope expression identifying the resource by a resource name and by at least one property associated with the resource, wherein the associated property includes at least one property name-property value pair, said property name-property value pair determining a list of conditions for access to the resource controlled by the second entity; and

a processor configured to execute computer-executable instructions for issuing from the centralized location to the first entity, responsive to [[a]] an authorization request from the first entity, the authorization data for a user based on a role associated with the user and for validating, in response to a request from the second entity, the authorization data issued to the first entity to provide access to the resource, said second entity granting to the first entity access to the resource according to the conditions determined by the property name-property value pair when the determined validation status indicates that the authorization data is valid.

Claim 29 (canceled).

Claim 30 (currently amended): The system of claim 28, wherein the processor is further configured to execute computer-executable instructions for evaluating the conditional scope expression to identify the resource.

Claim 31 (original): The system of claim 28, wherein the authorization data comprises a token.

Claim 32–35 (canceled).

Claim 36 (previously presented): The method of claim 1, wherein the first entity is an application program.

Claim 37 (previously presented): The method of claim 1, wherein the first entity is a computing device.

Claim 38 (currently amended): The method of claim 1, further comprising generating a signature based on the conditional scope expression identifying the resource, and wherein the validation information includes said generated signature.

Claim 39 (previously presented): The method of claim 1 wherein the validation information includes an expiration date.

Claim 40 (previously presented): The method of claim 1, wherein the validation information further includes a site identifier identifying the first entity.

Claim 41 (previously presented): The method of claim 1 wherein said validation request includes the issued authorization data and wherein said validating includes:

retrieving the validation information from the received authorization data;

evaluating the retrieved validation information; and

sending a response to the second entity indicating the validation status of the received authorization data responsive to said evaluating the retrieved validation information.